Volume 5, Issue 6

[state of the internet] / security

A Year in Review

Table of Contents

Letter from the Editor

Martin McKeay
Editorial Director

As 2019 comes to a close, we want to thank you, our readers, for continuing to support Akamai's State of the Internet /Security (SOTI) report. The team, and the report, have both evolved significantly this year, and we plan to continue to grow and evolve in the years to come. We want to be a report you return to for important research again and again.

Why does Akamai produce the SOTI report and produce security research in general?

From an internal standpoint, the SOTI report and its research are excellent marketing materials. Good research makes for good stories, and good stories drive awareness of what a company considers important. In some ways, the type of research any security company publishes is nearly as important to building their reputation as the types of products they sell.

Why does a global group of researchers believe in the value of research and publication? Most individual responses we've received can be boiled down to two motivators. First, being recognized as a leader and source of intelligence in your chosen field is nice, no matter who you are. Second, the work our teams are doing is important. The security field is still young, and every piece of information, every nugget of wisdom that contributes to global knowledge, is valuable.

For my team – the writers, data scientists, and editors who develop this report and so much more – our work is our passion. Together, we have more than four decades of experience in security. We realize just how much there is left to discover and how little of it is quantified. Working with our researchers lets us make a difference by making their work accessible and interesting to you.

The SOTI report was originally based solely on DDoS and web application attacks, but we've evolved the report to cover a wide range of pressing security issues. As Akamai continues its own evolution as a security company, the types of data we have available will only grow. We've already started plotting for 2020, in all senses of the word.

You, our readers, are important to us. Without you, this report wouldn't exist. Thank you for reading, and we hope you'll continue to find value in our reports in the coming year. We welcome your feedback and your questions.

12 Months of Akamai Research

The Important Stories of the Past 12 Months

Welcome to the sixth State of the Internet / Security (SOTI) report of the year. As the end of 2019 draws near, we want to look back and examine the research Akamai has done over the last 12 months. From the start of October 2018 through the end of September 2019, we pay particular attention to the research coming out of Akamai's Security Intelligence Response Team (SIRT). Additionally, we highlight a selection of the more important news stories that affected the security industry in the past year.

While it might seem cliché to say it's been an interesting year, it's still true. More than ever before, security stories have become increasingly important and are becoming part of mainstream news. With elections on the minds of most people in the United States, we expect security to play an even bigger role in the year ahead.

October 2018

What a month! It began with a data breach affecting millions of people on Facebook. A short while later, Bloomberg published a story centering on nation-state supply chain hacks. Every vendor in the story, as well as the U.S. Department of Homeland Security, refuted the claims, but Bloomberg stood firmly behind their reporting.

October was also a busy month for our security teams. Akamai's Ryan Barnett published a blog post on security response headers and why business leaders and security managers should care about them. One day later, Larry Cashdollar published an examination of the Luis phishing kit, including some of its evasion techniques.

Cashdollar also broke the news surrounding the jQuery file upload vulnerability (CVE-2018-9206). While the issue was addressed, forks of the code and recycled usage spread its impact across other codebases. This meant the issue had the potential to affect 7,800 projects. In a follow-up post, Cashdollar tested 1,000 forked projects using the jQuery code, and discovered 970 of them were vulnerable.

With elections on the minds of most people in the United States, we expect security to play an even bigger role in the year ahead.

November 2018

November started off with word that the Library of Congress and the U.S. Copyright Office had added exemptions to the Digital Millennium Copyright Act (DMCA). One exemption allows researchers to expose flaws in software without fear of criminal prosecution. This news was followed by reports that some 60 million U.S. payment cards had been compromised between 2017 and 2018, and 93% of them were EMV enabled.

Around this time, Akamai's Kaan Onarlioglu published a blog discussing third-party vulnerability assessments on the Akamai Intelligent Edge Platform and the existence of false-positive results that could lead to confusion. Soon after, Ryan Barnett published an in-depth report on steps to take to protect yourself from Magecart attacks, and Or Katz published a detailed look into a phishing scam with 78 different variations. Magecart software continues to be a significant threat as we close out 2019, in large part because of the vulnerabilities both in the software and in third-party plugins used in many sites.

December 2018 / January 2019

Toward the end of 2018, the publication and research teams also put the finishing touches on the first State of the Internet / Security report for 2019, published on January 30. It seems researchers, and even criminals, took much of December off.

Before the SOTI report hit the presses, Larry Cashdollar published a blog centered on the ThinkPHP vulnerability (CVE-2018-20062), which was discovered while he was researching Magecart skimming attacks. Lukasz Orzechowski followed that post by blogging about an experiment with Computer-Aided Translation (CAT) tools. Translations between languages are hard, especially when you're translating a computer script with technical writing.

State of the Internet / Security: Volume 5, Issue 1

DDoS and Application Attacks

This issue explored mental health, with a guest essay by Amanda Berlin. Since January, the number of Mental Health Hackers workshops at security conferences has grown across the United States.

We took a deep dive into an incident that, at first glance, looked like a massive DDoS attack, with more than 4 billion requests, across more 15,582 IP addresses. However, "the attack that wasn't" turned out to be a faulty application.

We also explored the topic of retail bots and how All-in-One (AIO) applications can seriously impact online sales and promotions. While not all bots are bad, some can certainly be more trouble than they're worth.

TL;DR

- Mental health issues cost U.S. businesses more than **$190 billion** a year in lost earnings.
- Sometimes an "attack" isn't exactly what it first appears to be. Experts in Akamai's SOCC saw **4 billion requests** impact a major website and dug into the real cause.
- **Bots are big money for attackers**, and they're constantly evolving to circumvent new defenses. One attacker offered $15,000 in his search for developers with experience in targeting specific company defenses.

February 2019

February was cold, and so was the news cycle. However, there were some interesting stories, including a case in which someone filed a lawsuit against Apple for forcing two-factor authentication on user accounts.

An incident notification letter filed with the Vermont Attorney General's Office [PDF] also drew attention. The incident in question was a credential stuffing attack that targeted TurboTax users, rather than a breach of Intuit systems. Examples like this are one reason why multi-factor authentication and credential stuffing were themes Akamai followed throughout 2019. Another reason is the sheer volume of credential stuffing attacks Akamai continues to see.

Just before the second issue of the SOTI report was published this month, Larry Cashdollar published a blog post examining the use of Google Translate in phishing attacks against Facebook. LPT: Don't poke researchers with phishing attempts, as they make their living digging into strange and unusual patterns.

Multi-factor authentication and credential stuffing were themes Akamai followed throughout 2019.

State of the Internet / Security: Volume 5, Issue 2

Retail Attacks and API Traffic

This was the first time this year when Akamai dug into our credential stuffing data. At the time this report was filed, Akamai had observed 10 billion credential stuffing attempts against the retail sector between May and December 2018. The report also dug into AIO bots in the retail sector, API security, and potential IPv6 problems.

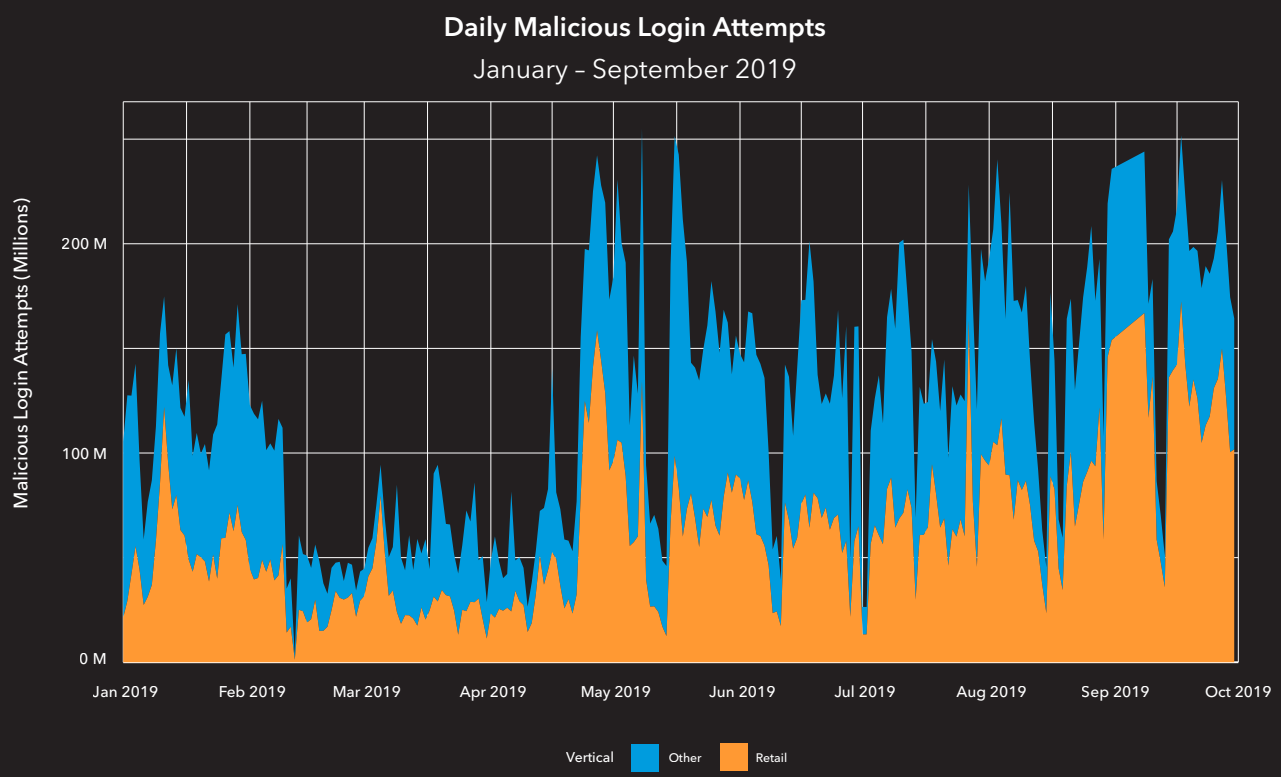
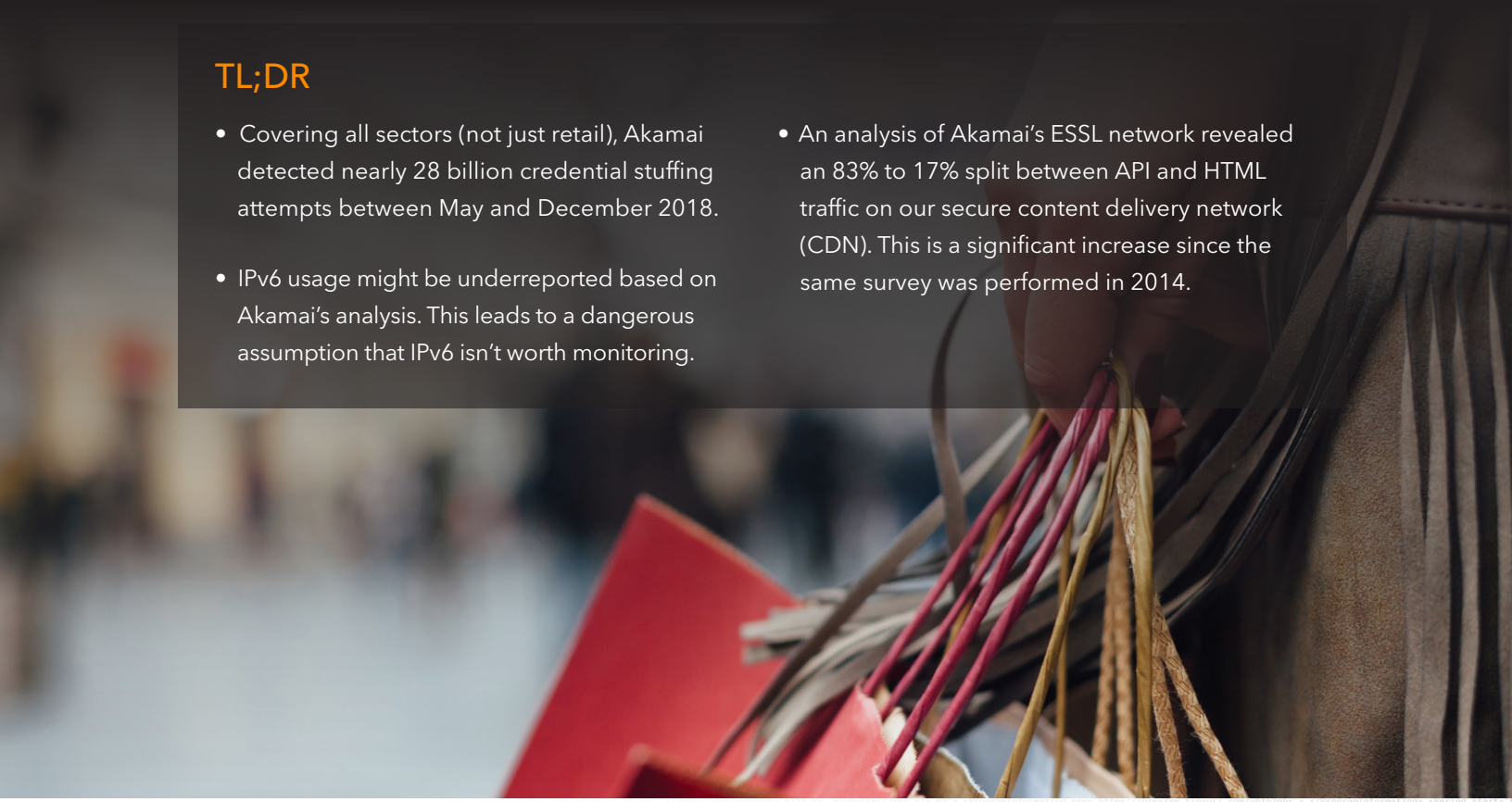


Fig. 1 (Update of chart published in issue 2) – Credential stuffing continues to largely target the retail industry, with 16.5 billion attempts in the first nine months of 2019, compared with 11.5 billion in the last nine months of 2018

TL;DR

- Covering all sectors (not just retail), Akamai detected nearly 28 billion credential stuffing attempts between May and December 2018.
- IPv6 usage might be underreported based on Akamai's analysis. This leads to a dangerous assumption that IPv6 isn't worth monitoring.
- An analysis of Akamai's ESSL network revealed an 83% to 17% split between API and HTML traffic on our secure content delivery network (CDN). This is a significant increase since the same survey was performed in 2014.



March 2019

When discussing credential stuffing attempts, one of the key themes is the use of easily guessed or weak passwords. In addition, far too many users recycle their passwords across multiple networks and services. Early in March, stories about Comcast's Xfinity Mobile phone service having a default PIN of 0000 on customer accounts came to light. This story circulated shortly after rapper and business mogul Kanye West was shown to have set the password on his iPhone X to 000000.

Outside of the news cycle, Akamai's Jonathan Respeto published a blog on using Capture the Flag programs to promote continuous training within the Security Operations Command Center (SOCC).

April 2019

April arrived, and as the team recovered from the RSA Conference, news of a trio of WordPress zero-day vulnerabilities started to spread online, leading to a number of website compromises. Akamai researchers often observe that criminals use compromised websites to host phishing kits. This also helps with evasion; a legitimate but compromised website isn't likely to raise suspicions or trigger endpoint defense alarms.

In other vulnerability news, Larry Cashdollar published a blog that warned about multiple vulnerabilities in Magento. The advisory, published to bring attention to the issue, called out more than 30 vulnerabilities in the platform, including one that had a working proof-of-concept at the time. Later in the month, researcher Yael Daihes published a blog with Craig Sprosts about adding real-world DNS data to deep learning models in order to increase effectiveness.

State of the Internet / Security: Special Media Edition

Credential Stuffing – Attacks and Economies

Released on April 8, 2019, this special edition of the SOTI report was published with the media audience at the National Association of Broadcasters (NAB) conference in mind. Akamai's Patrick Sullivan presented data and intelligence from the report at the NAB Cybersecurity & Content Protection Summit.

One of the more interesting points in this report was that three of the largest credential stuffing attacks against streaming services in 2018, which ranged in size from 133 million to 200 million attempts, took place soon after data breaches were reported, meaning the attackers were trying to take advantage of newly obtained credentials.

May 2019

Highlights from May include patches from Cisco that addressed serious router vulnerabilities and Baltimore's ransomware difficulties and recovery efforts. Ransomware has been a common theme in the past year, and the use of ransomware shows little evidence of abating.

Akamai's Amiram Cohen, with additional research by Or Katz, published a detailed look into the 16Shop phishing kit, which targets Apple users. The kit itself is advanced, constantly updated, and uses a number of evasion techniques. The Akamai Threat Research Team also published a blog related to Cipher Stunting, which is a growing threat that involves randomizing SSL/TLS signatures in an attempt to evade detection.

June 2019

June is usually a busy month for security news, and this year was no exception. There were attacks against WordPress plugins, data breaches, and incidents involving POS malware in 102 Checkers and Rally's restaurants across 20 states. In lighter news, a study was published that claimed cognitive bias has an effect on security decisions.

Larry Cashdollar and Steve Ragan started the month by blogging about identifying vulnerabilities in phishing kits, which, if exploited, could lead to additional problems for server administrators. Or Katz, who presented during Akamai's Edge World conference, also published blogs related to phishing kit evasion techniques and phishing analytics. Cashdollar also published two additional blogs that month. The first, on June 13, addressed 26 infection vectors in the newest (at the time) version of Echobot. At the end of the month, he posted about a bot named Silex that bricked systems once infected.

State of the Internet / Security: Volume 5, Issue 3

Web Attacks and Gaming Abuse

This edition of the SOTI report centered on gaming and the criminal economy behind it. Gaming is a hot target, and criminals have multiple paths available to target gamers and the companies behind some of the web's hottest gaming titles. Data wise, the report noted that there were 12 billion credential stuffing attacks against gaming websites between November 2017 and March 2019; across all industries, there were more than 55 billion credential stuffing attacks during the same time frame. Web applications were

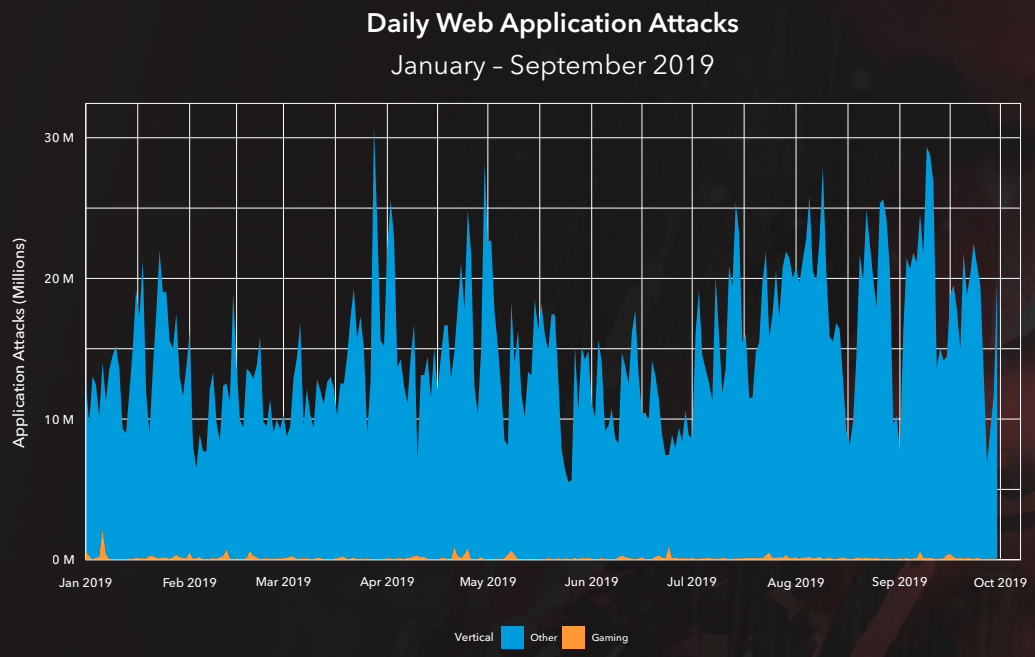


Fig. 2 – Although gaming organizations are only the target of a small percentage of the attacks Akamai sees, they have still been targeted by more than 35 million attempts in the first nine months of 2019

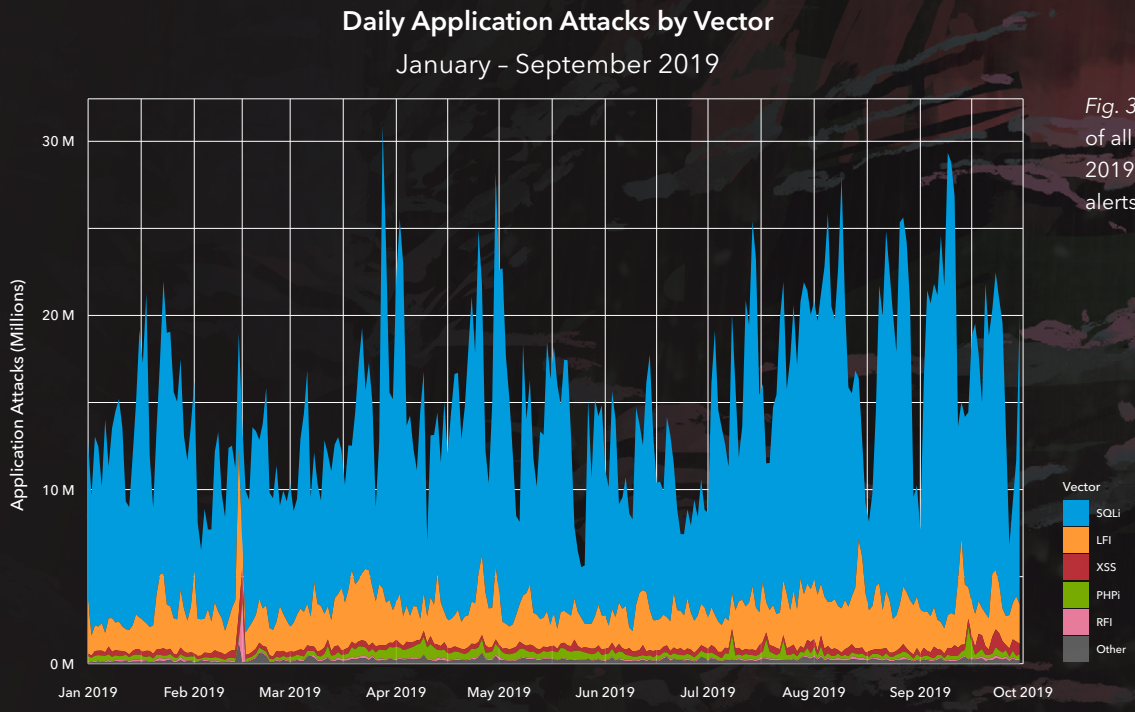


Fig. 3 – SQLi attacks account for 77% of all application attacks so far in 2019, creating more than 3.1 billion alerts on Akamai's platform

TL;DR

- Akamai observed 55 billion credential stuffing attacks over 17 months, and 12 billion of them were aimed directly at the gaming industry.
- SQLi is the top threat when it comes to web application risks, accounting for nearly two-thirds of all attacks.
- Overall, the United States is still the top source for credential stuffing, followed by Russia. But when looking at gaming data alone, Russia is the number one source.

July 2019

In July, most people in the security industry, including many of us at Akamai, were gearing up for events in Las Vegas. Security companies talk a lot about risks and attack surfaces. One of the most common attack surfaces is the browser; so when news that Germany's *Bundesamt für Sicherheit in der Informationstechnik* (BSI) was drafting guidelines for browser security, people took notice.

In-house, on the research side of things, Akamai's Chad Seaman published a blog on SYN-ACK attacks. Lior Lahav and Asaf Nadler discussed recent changes to the domain generation algorithm (DGA) for Pykspa v2, followed by a second post that explored DGA mitigations. Finally, Larry Cashdollar published a blog on July 29 about criminals leveraging Local File Inclusion (LFI) vulnerabilities in their phishing campaigns.

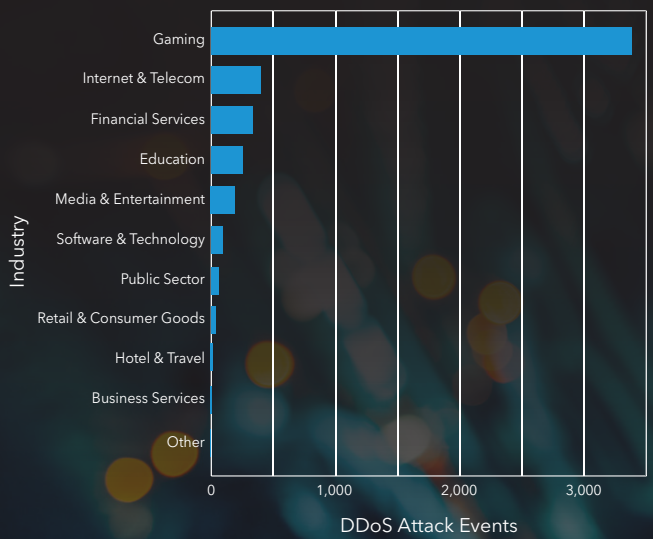
State of the Internet / Security: Volume 5, Issue 4

Financial Services Attack Economy

This edition of the SOTI report explored how the attacks and tools being used against financial services are part of a larger, more complex ecosystem. The report looked inside criminal markets and examined how they target financial organizations, as well as what happens after a successful attack.

DDOS – Attack Events

January 2019 – September 2019



DDoS – Unique Targets

January 2019 – September 2019

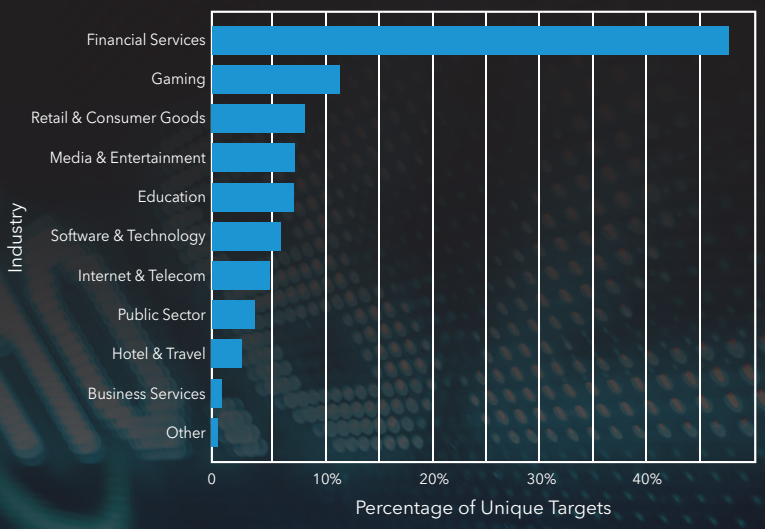


Fig. 4 (Update of chart published in issue 4) – DDoS attacks most often target gaming companies, but attacks against the financial services industry are much more dispersed across multiple targets

TL;DR

- Half of all unique organizations impersonated by phishing domains were in the financial services sector, according to Akamai data.
- More than 6% of the malicious login attempts globally targeted the financial sector.
- 94% of the attacks against the financial sector came from SQLi attacks, LFI, Cross-Site Scripting (XSS), and OGNL Java Injections.

August 2019

In early August, Black Hat, DEF CON, and BSides Las Vegas were taking place, and many of the early headlines were part of what journalist Violet Blue calls "Infosec Clickbait Season." But the news item that got the most buzz wasn't even security-related – it was about a man wearing a TV on his head, who was observed on camera leaving TVs on porches in Virginia. After narrowly avoiding a plague of locusts in Las Vegas, those who attended Black Hat were told they might have been exposed to measles if they were in the area between August 3 and 5.

In the research department, Akamai's Or Katz published a blog about phishing scams targeting vacation hotspots, and Larry Cashdollar wrote about XMR cryptocurrency mining software being spread in the wild.

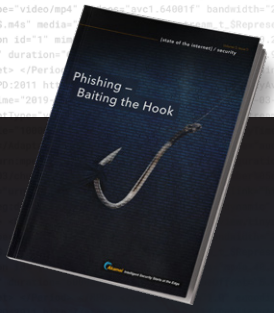
September 2019

Akamai's Jonathan Respeto and Chad Seaman published a blog discussing a new DDoS vector that can hit 35/Gbps. The vector, which leverages a UDP amplification technique known as WS-Discovery (WSD), can be used to get amplification rates of up to 15,300%.

State of the Internet / Security: Special Media Edition

Media Under Assault

Released in support of the IBC media, entertainment, and technology show, this special edition of the SOTI report continued the trend of following credential stuffing activities, with a detailed look at how they impact media and technology companies. Collectively, from January 2018 until June 2019, Akamai recorded more than 61 billion credential stuffing attempts and more than 4 billion web application attacks.



State of the Internet / Security: Volume 5, Issue 5

Phishing: Baiting the Hook

The last research-focused SOTI report of the year focused on phishing, and the economics and methods that support it. This issue also includes, for the first time ever, data from Akamai's own internal tracking on phishing attempts that targeted our employees.

TL;DR

- 60% of the phishing kits monitored by Akamai were active for 20 days or less.
- High technology is the top industry targeted by phishing, according to Akamai's data.
- Microsoft, PayPal, DHL, Dropbox, DocuSign, and LinkedIn are all top phishing targets, according to Akamai's monitoring.

News Sources

In addition to the linked sources in this report, below is a list of some news sources that the contributors to this report read on a regular basis for insightful analysis and industry coverage.

- Violet Blue
- Zack Whittaker
- Dark Reading
- Ars Technica
- Motherboard
- CyberScoop
- CSO Online
- WIRED
- TechCrunch
- ZDNet
- SecurityWeek
- Forbes

Looking Forward

'Tis the season of "security predictions." We hate security predictions.

Futurists and science fiction writers make predictions about the future. Gene Roddenberry and his creation *Star Trek* have become staples of the collective consciousness and have either predicted or led to the creation of many of the gadgets we use daily, such as cell phones and Bluetooth headphones. But we're security professionals, not futurists, and we have never been able to make predictions a year in advance with any accuracy.

May you live in interesting times.

–Ancient Chinese Curse

What we can do is look at the data we have today and extrapolate trends from that. You might wonder how that differs from a prediction, to which the answer is, primarily, perspective. Both extrapolation and prediction are attempts to find emergent trends, but prediction has a more sensational bias.

When someone is asked for a prediction, there's an assumed need for the response to be new and different from what others have pointed to; extrapolation is based more on real-world trends. Yes, it's splitting hairs and pedantic, but that level of specificity is what we should be expecting from researchers and editors.

So, what can we extrapolate from the trends of 2019? First, credential abuse, phishing, and exploitation of vulnerabilities in popular systems will continue to grow. This is an easy call to make, but the difference is that we're seeing professional weaponization of these attacks. If anything, we're going to see more weaponization and more diversity in attacks.

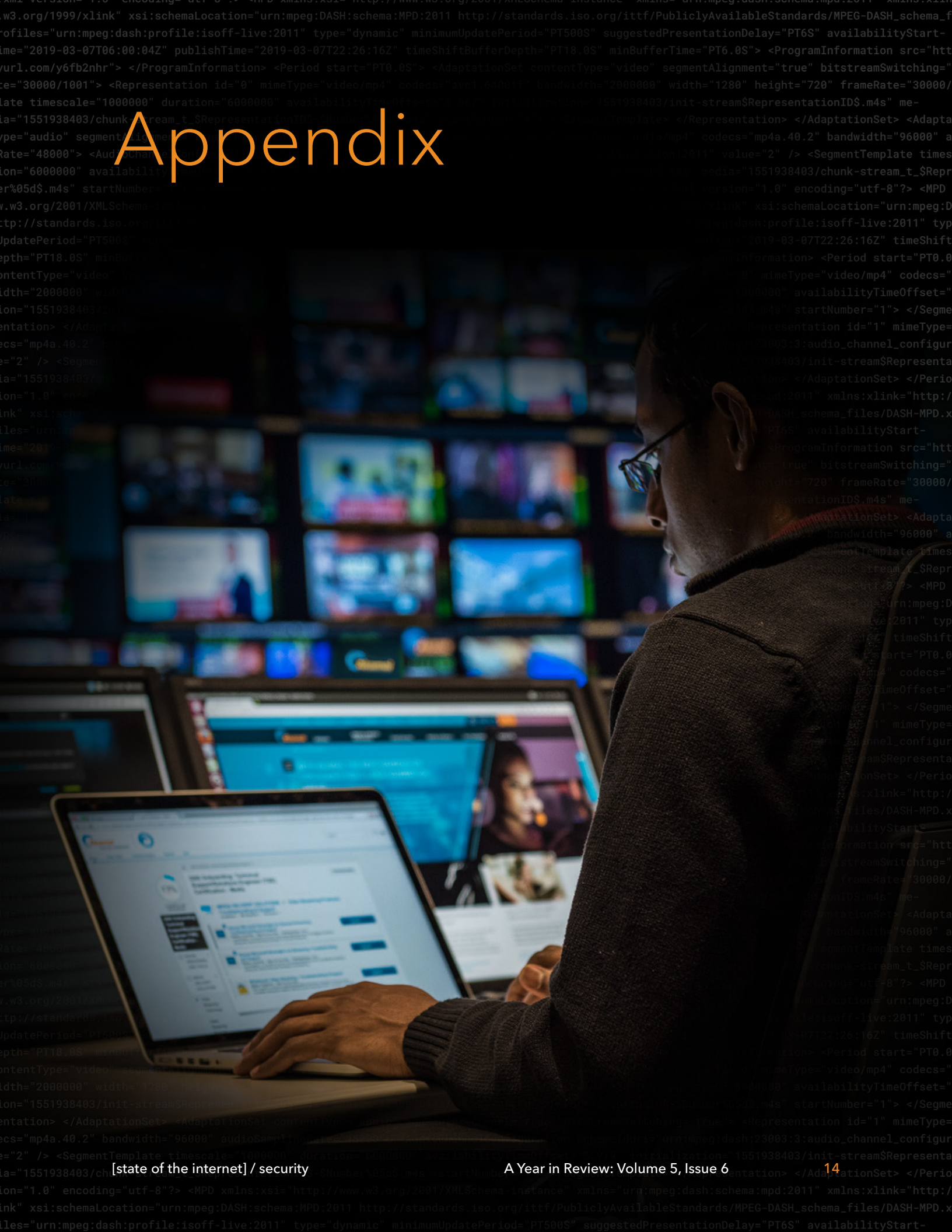
A decade ago, vulnerabilities were usually found by a criminal, then incorporated into attacks. Five years ago, it became much more common to see professional teams of criminals who discovered and developed attack software. The trend now is an overlap between criminal developers and the advanced persistent threat (APT), or nation-state actors, to create a steady stream of zero-day tools targeting specific organizations and individuals.

This is not merely speculation. In early October, the NSA went to the extreme of issuing a warning that known nation-state actors were targeting vulnerable VPN platforms. There are multiple other communication channels from which such advisories would normally come, so this shows that the NSA views this as a clear and present danger.

We're moving away from an era when the security advisors in a company were viewed as alarmists, to one where even we are sometimes caught off guard by the severity and impact of attacks. Esoteric topics about security that used to be the realm of specialists and technologists are now part of the daily news cycle and collective consciousness. Many of the predictions from a decade ago are now becoming real, even if the threats look nothing like what most of us expected.

One prediction we can make is that 2020 will be interesting.

Appendix

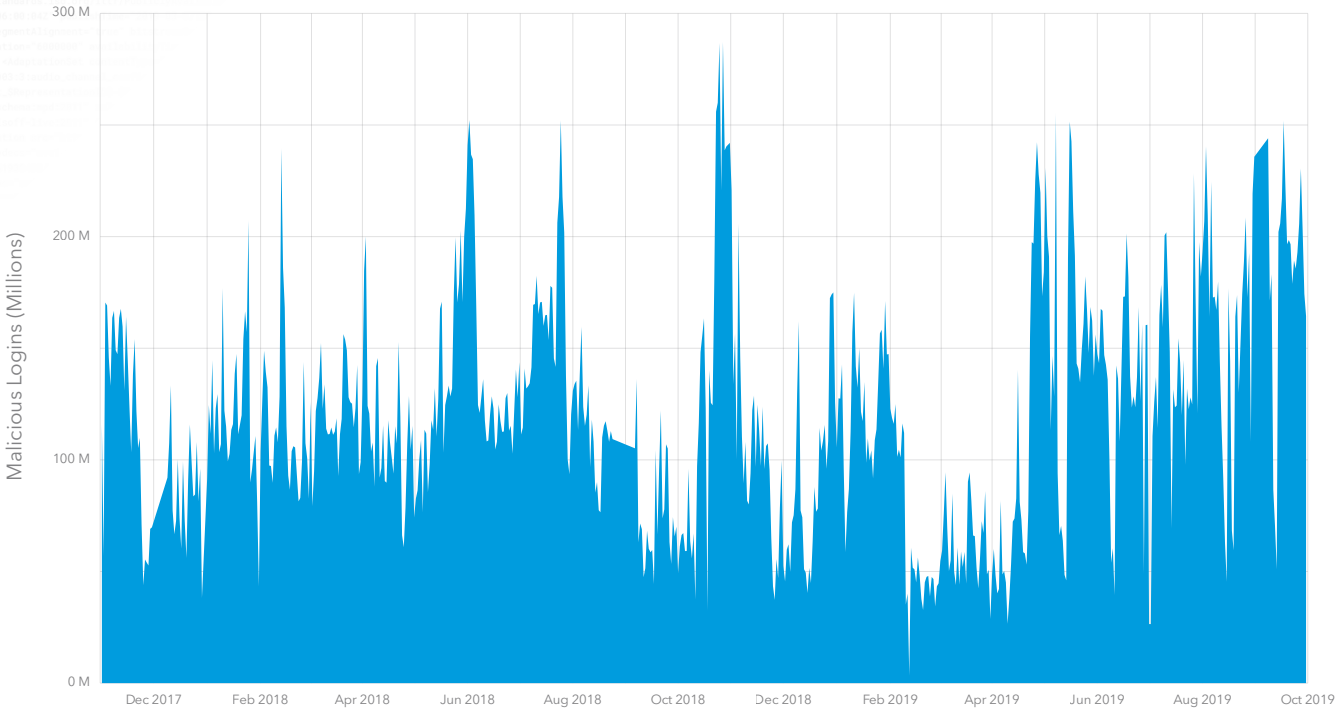


Important Updates of Our Big Stories

The following plots are updates from work in previous issues of volume 5 of the State of the Internet / Security report. We are providing them for readers as supplemental information with minimal supporting text and explanation. All plots and tables span the time from November 2017 until September 2019.

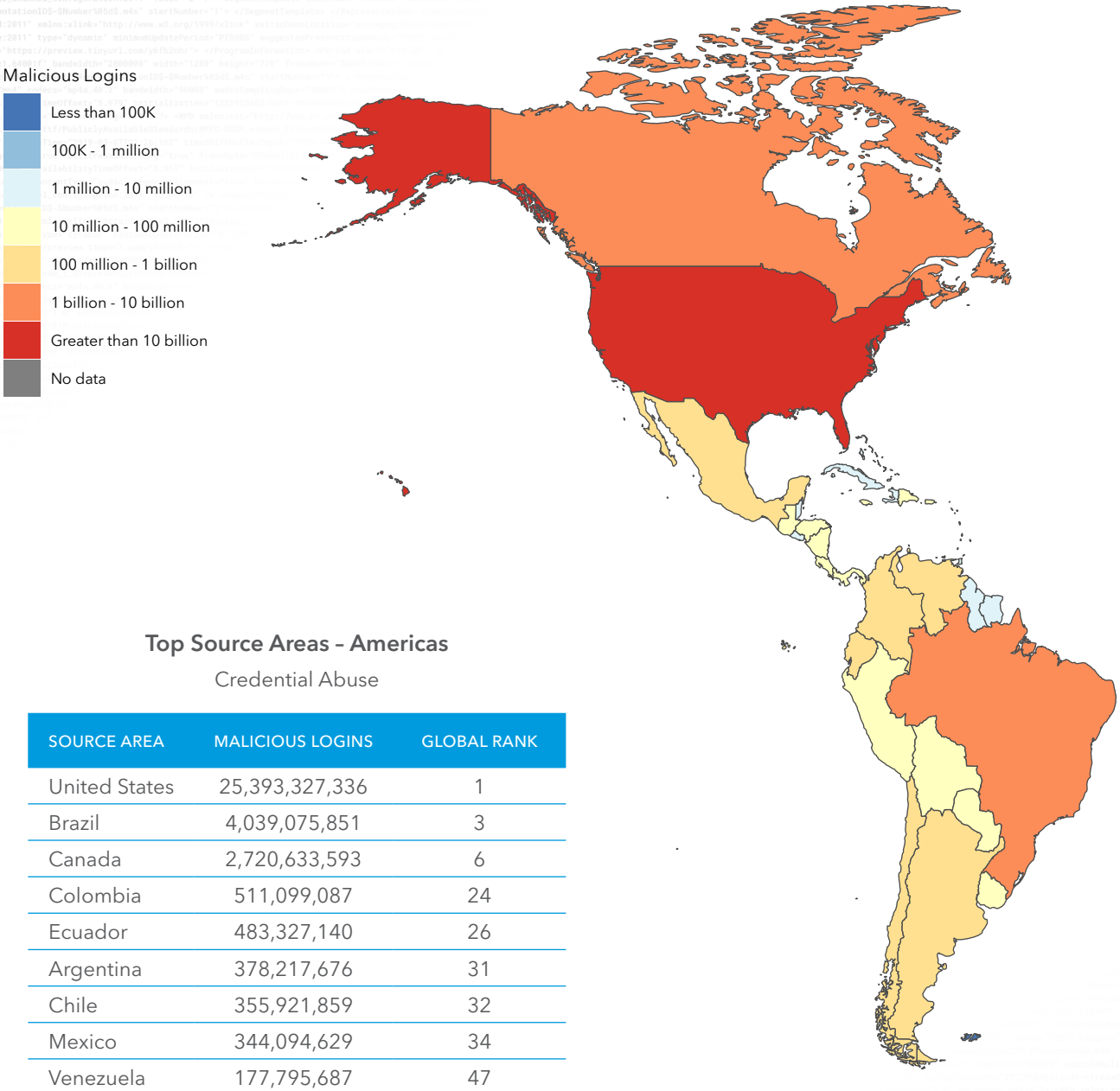
Daily Malicious Login Attempts

November 2017 – September 2019



Credential Abuse Attack Sources – Americas

November 2017 – September 2019



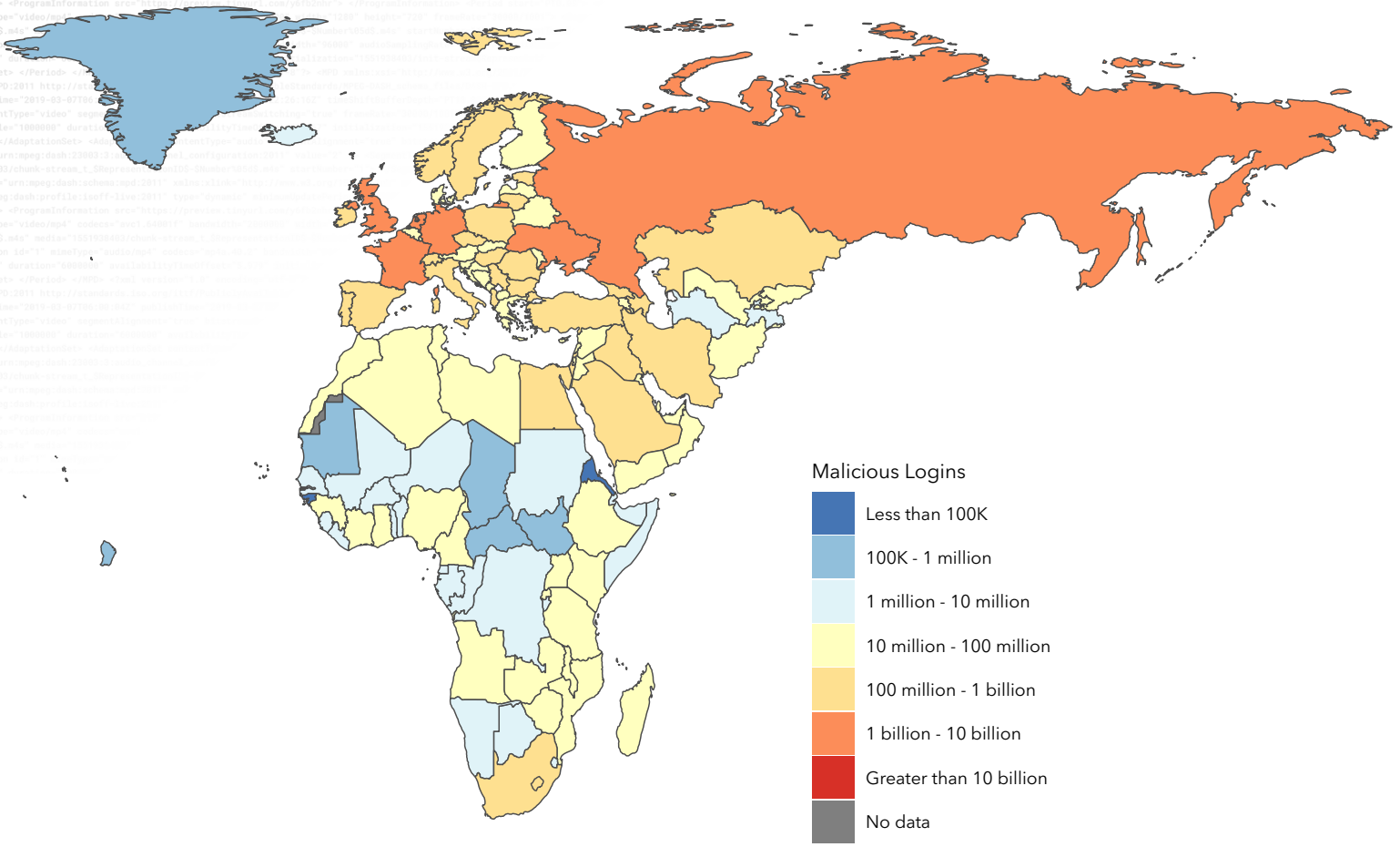
Top Source Areas – Americas

Credential Abuse

SOURCE AREA	MALICIOUS LOGINS	GLOBAL RANK
United States	25,393,327,336	1
Brazil	4,039,075,851	3
Canada	2,720,633,593	6
Colombia	511,099,087	24
Ecuador	483,327,140	26
Argentina	378,217,676	31
Chile	355,921,859	32
Mexico	344,094,629	34
Venezuela	177,795,687	47
Peru	90,149,099	65

Credential Abuse Attack Sources – EMEA

November 2017 – September 2019



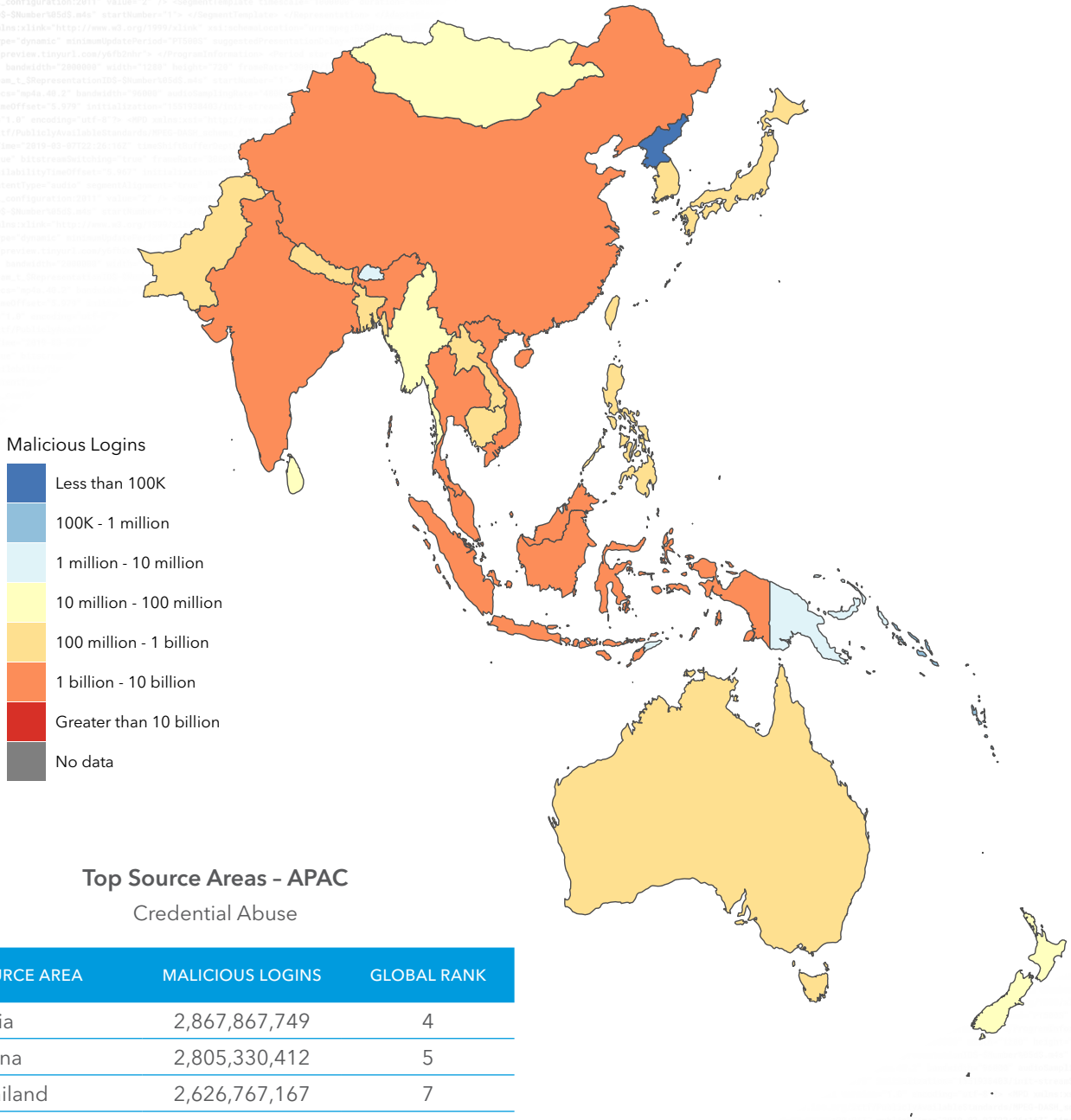
Top Source Areas – EMEA

Credential Abuse

SOURCE AREA	MALICIOUS LOGINS	GLOBAL RANK
Russia	6,114,186,048	2
Germany	2,129,388,432	10
France	2,081,826,451	11
Netherlands	1,723,393,319	12
United Kingdom	1,559,263,043	14
Ukraine	1,097,729,730	16
Italy	879,866,419	17
Estonia	652,938,763	21
Poland	571,536,319	23
Spain	490,167,797	25

Credential Abuse Attack Sources – APAC

November 2017 – September 2019



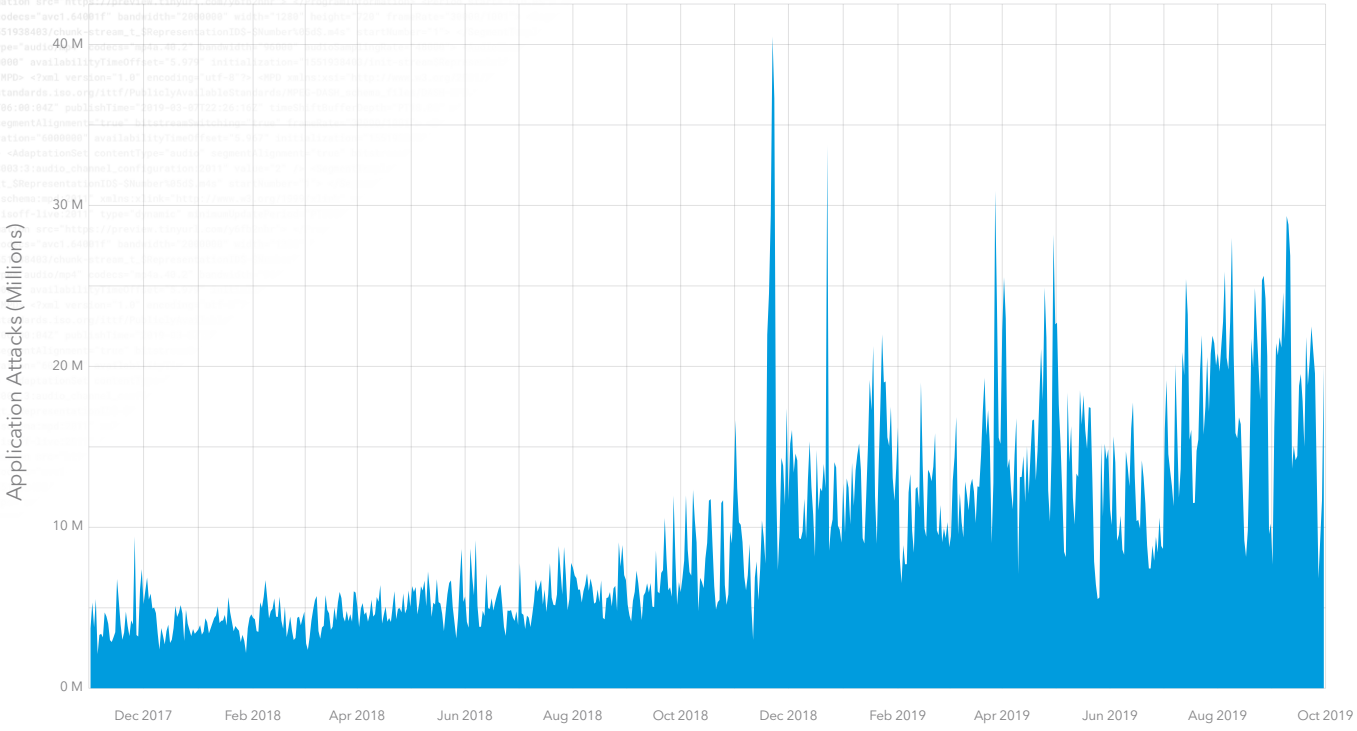
Top Source Areas – APAC

Credential Abuse

SOURCE AREA	MALICIOUS LOGINS	GLOBAL RANK
India	2,867,867,749	4
China	2,805,330,412	5
Thailand	2,626,767,167	7
Indonesia	2,328,720,242	8
Vietnam	2,166,055,670	9
Singapore	1,568,843,384	13
Malaysia	1,547,306,924	15
Japan	845,793,217	18
Taiwan	817,736,419	19
South Korea	737,126,412	20

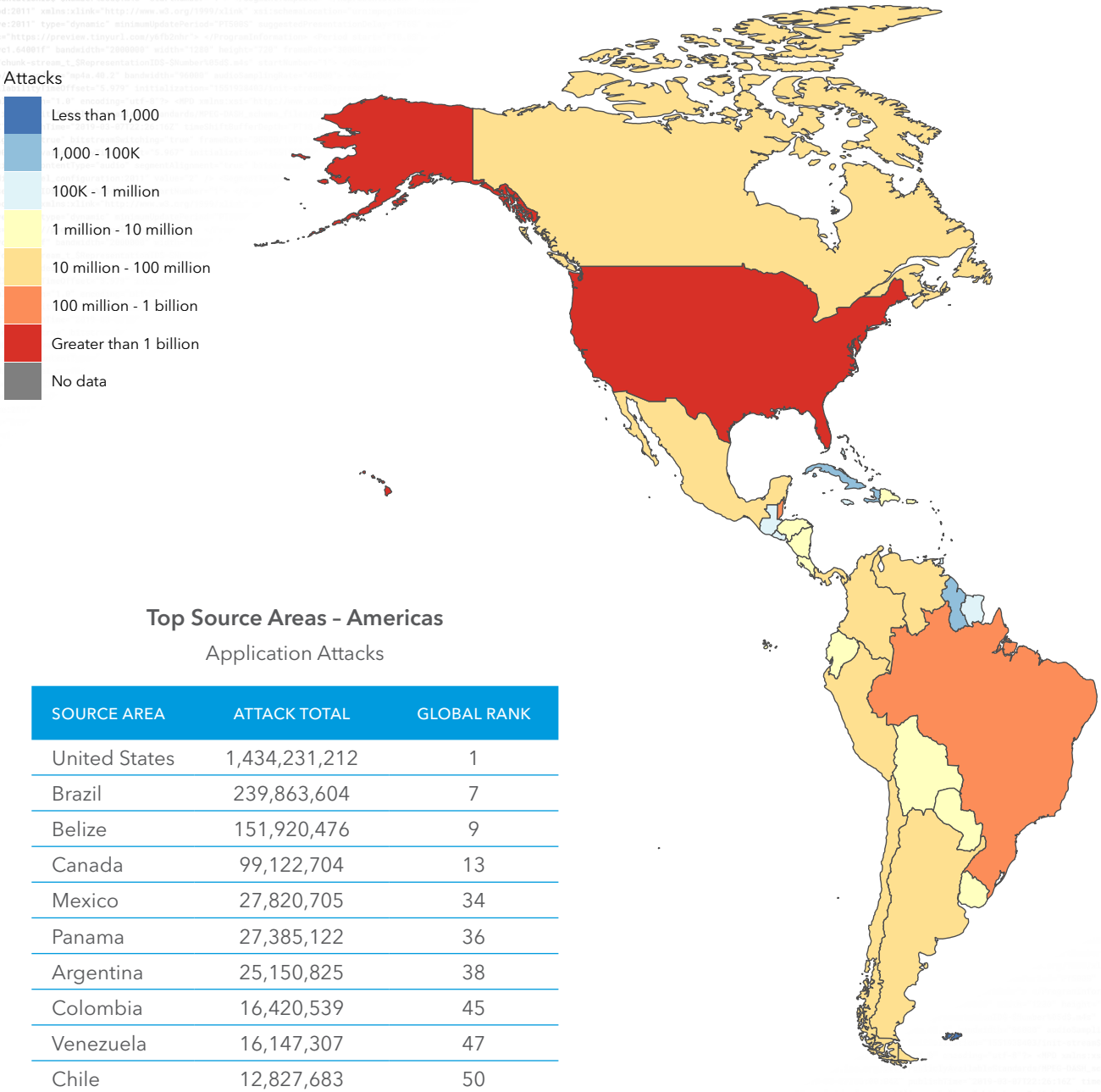
Daily Web Application Attacks

November 2017 – September 2019



Web Application Attack Sources – Americas

November 2017 – September 2019



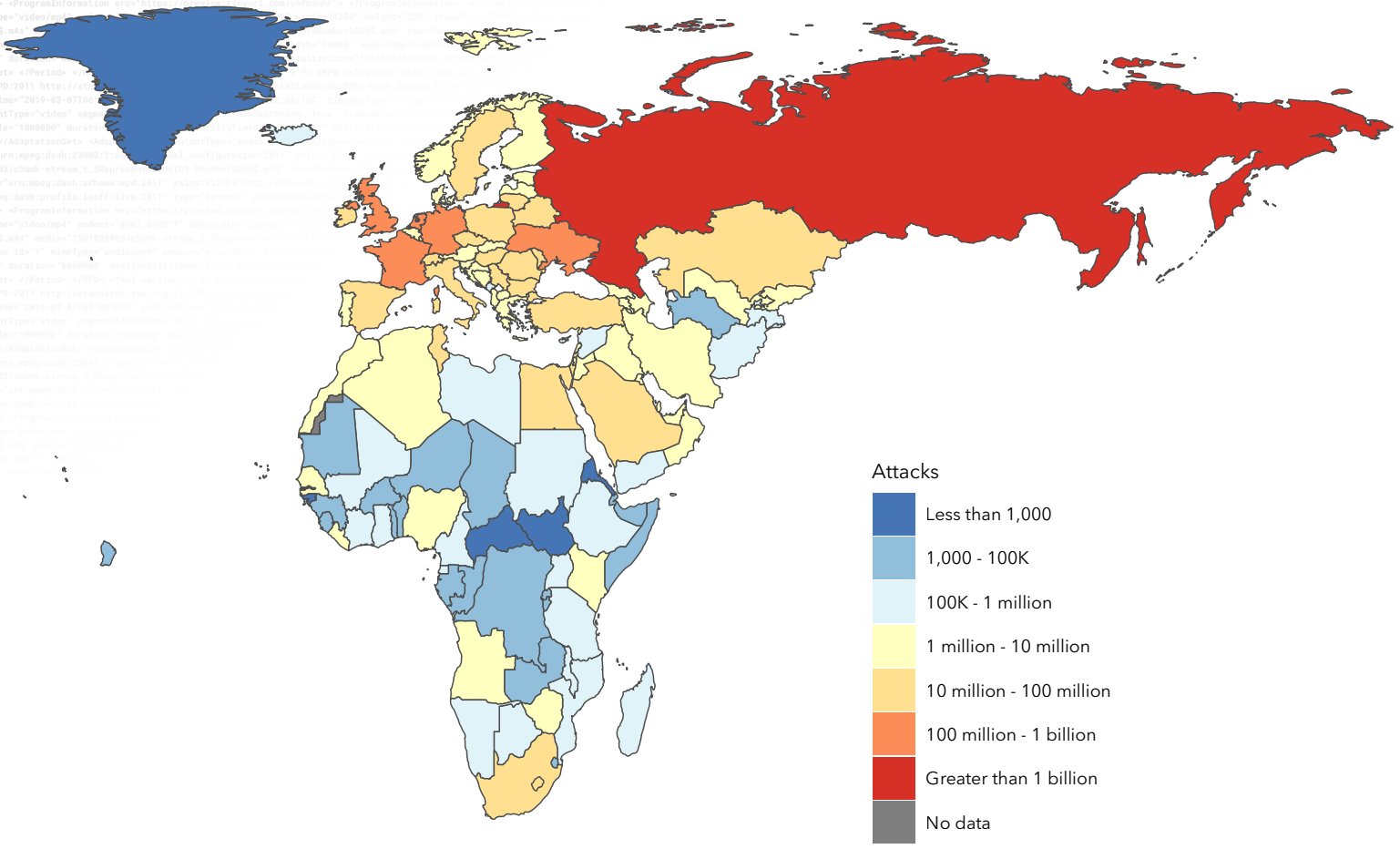
Top Source Areas – Americas

Application Attacks

SOURCE AREA	ATTACK TOTAL	GLOBAL RANK
United States	1,434,231,212	1
Brazil	239,863,604	7
Belize	151,920,476	9
Canada	99,122,704	13
Mexico	27,820,705	34
Panama	27,385,122	36
Argentina	25,150,825	38
Colombia	16,420,539	45
Venezuela	16,147,307	47
Chile	12,827,683	50

Web Application Attack Sources – EMEA

November 2017 – September 2019



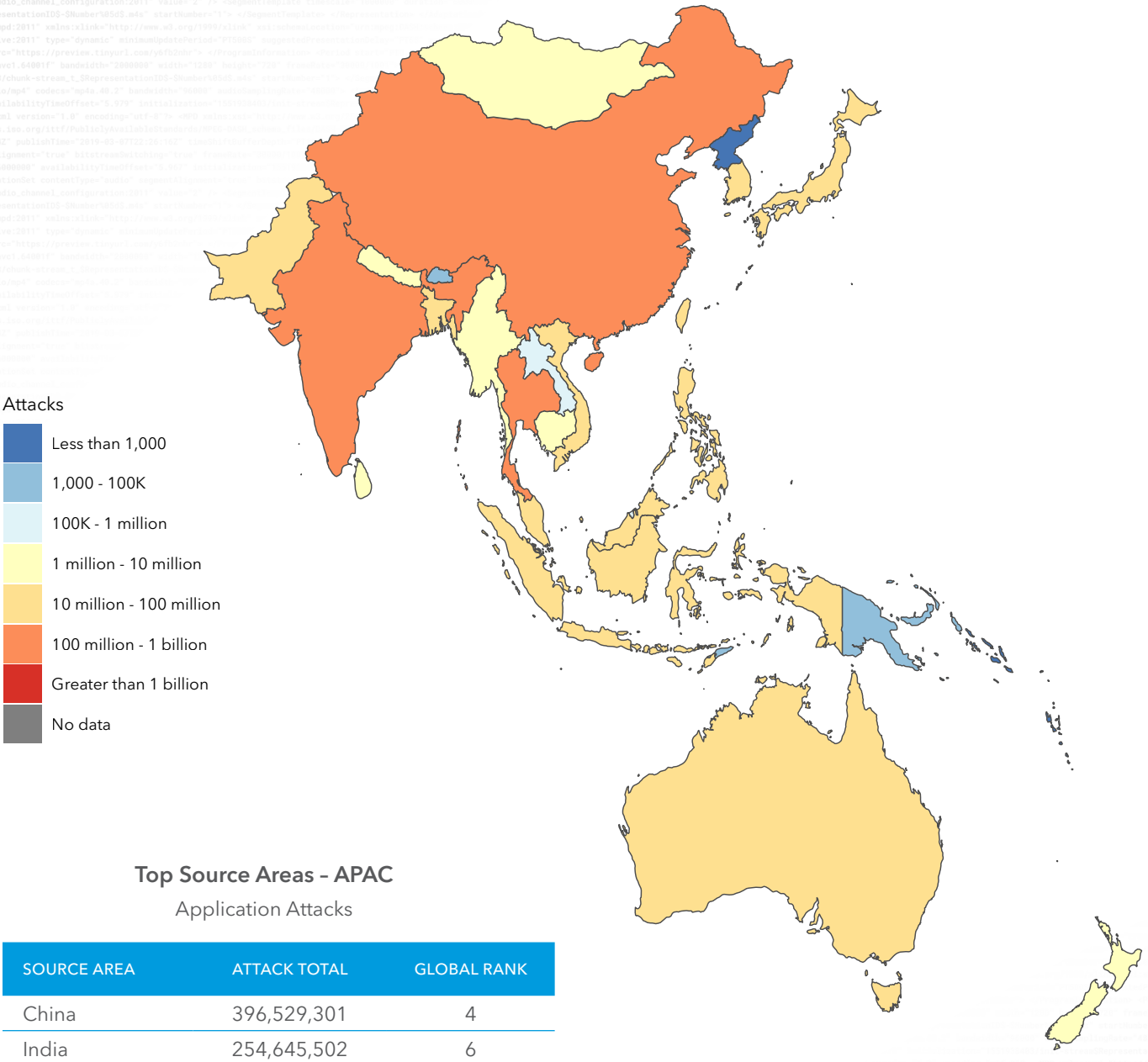
Top Source Areas – EMEA

Application Attacks

SOURCE AREA	ATTACK TOTAL	GLOBAL RANK
Russia	1,093,219,355	2
Netherlands	414,257,266	3
Ukraine	288,844,085	5
Germany	200,129,170	8
France	148,147,042	10
United Kingdom	141,076,862	11
Ireland	93,537,634	14
Turkey	88,376,455	16
Romania	69,929,767	20
Italy	52,615,647	24

Web Application Attack Sources – APAC

November 2017 – September 2019



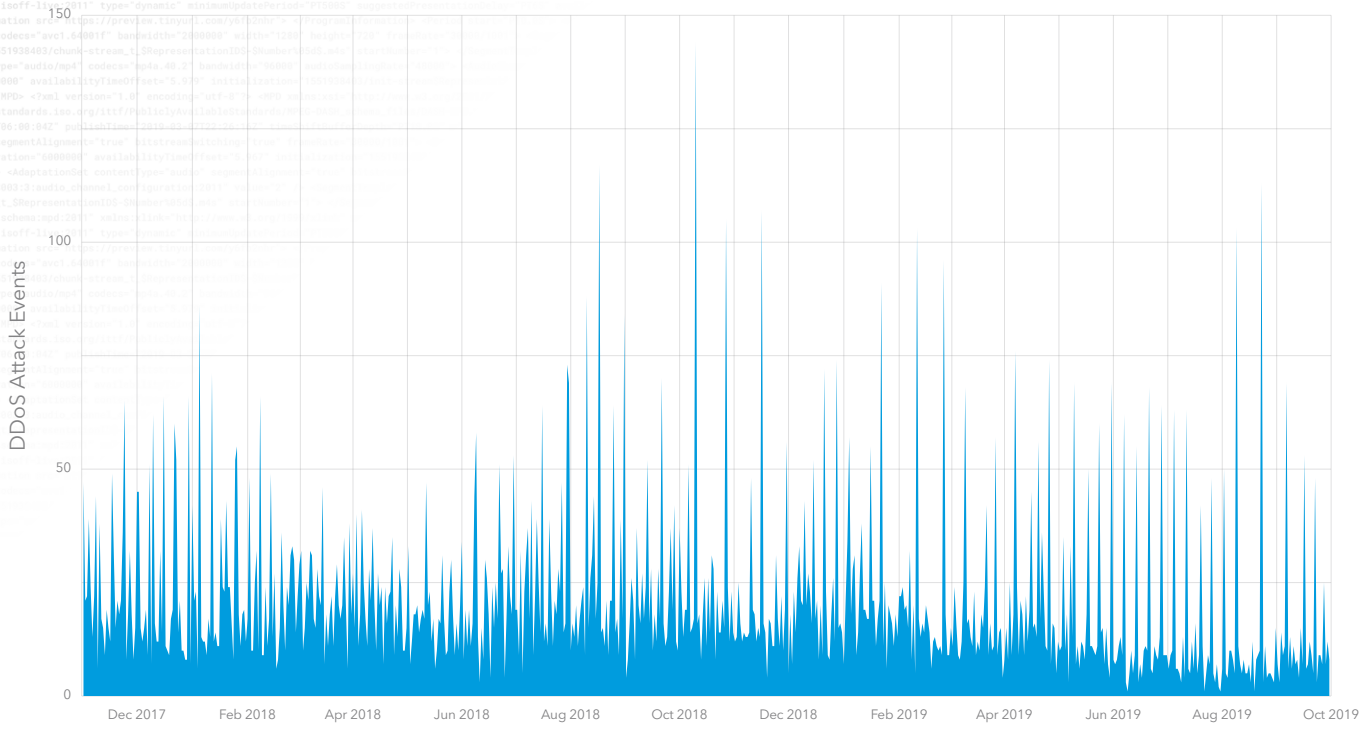
Top Source Areas – APAC

Application Attacks

SOURCE AREA	ATTACK TOTAL	GLOBAL RANK
China	396,529,301	4
India	254,645,502	6
Thailand	120,351,975	12
Singapore	91,057,766	15
Indonesia	83,441,813	17
Japan	76,396,164	18
Vietnam	63,455,055	22
Taiwan	57,639,687	23
Hong Kong	49,977,066	25
South Korea	43,552,997	27

Daily DDoS Attack Events

November 2017 – September 2019



Credits

State of the Internet / Security Contributors

VOLUME 5, ISSUE 1

Ben Tang
Data Scientist

Elad Shuster
Senior Lead Security Researcher

Chad Seaman
Security Intelligence Response Team, Senior II

Larry Cashdollar
Security Intelligence Response Team, Senior II

Moshe Zioni
Threat Research, Director

Gabriel Bellas
Practice Manager, Global Services

Guest Author: Amanda Berlin
Mental Health Hackers

VOLUME 5, ISSUE 2

Tony Lauro
Senior Manager, Security Strategy

Moritz Steiner
Principal Architect

Kyle Schomp
Performance Engineer, Senior II

Rami Al-Dalky
Intern

VOLUME 5, SPECIAL MEDIA EDITION: CREDENTIAL STUFFING – ATTACKS AND ECONOMIES

Shane Keats
Director of Global Industry Marketing, Media, and Entertainment

Steve Ragan
Researcher, Senior Technical Writer

Martin McKeay
Editorial Director

VOLUME 5, ISSUE 3

Elad Shuster
Senior Lead Security Researcher

Lydia LaSeur
Data Scientist

Tim April
Principal Architect

Steve Ragan
Senior Technical Writer

Martin McKeay
Editorial Director

VOLUME 5, ISSUE 4

Elad Shuster
Senior Lead Security Researcher

Or Katz
Principal Lead Security Researcher

Tim April
Principal Architect

State of the Internet / Security Contributors

VOLUME 5, ISSUE 4 (CONT.)

Lydia LaSeur
Data Scientist

Steve Ragan
Senior Technical Writer

VOLUME 5, SPECIAL MEDIA EDITION: MEDIA UNDER ASSAULT

Omri Hering
Data Analyst Senior

Lydia LaSeur
Data Scientist

VOLUME 5, ISSUE 5

Eric Kloster
Engineering Director

Lorenz Glaser
Senior II Security Engineer

Or Katz
Principal Lead Security Researcher

Lydia LaSeur
Data Scientist

Paul O'Leary
Principal Data Scientist,
Threat Intelligence Engineering

EDITORIAL TEAM FOR VOLUME 5, ISSUES 1 - 6

Martin McKeay
Editorial Director

Amanda Fakhreddine,
Managing Editor, Senior Technical Writer

Steve Ragan
Senior Technical Writer

Lydia LaSeur
Data Scientist

CREATIVE AND MARKETING TEAM FOR VOLUME 5, ISSUES 1 - 6

Benedikt Van Holt
Art Direction

Brendan John O'Hara
Graphic Design

Georgina Morales Hampe
Project Management

Kylee McRae
Program Management

Murali Venukumar
Program Management